Sandy Bacik

From: Sandy Bacik
Sent: Friday, February 10, 2012 6:29 AM
To: csctgarchi@nist.gov
Subject: CSWG Architecture minutes from 20120209

CSWG Architecture twiki: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CsCTGArchi
Chair: Sandy Bacik (sandy.bacik@enernex.com)

20120209 Minutes

1. Current Tasks
    a. To catch everyone up on our consensus work, a summary pdf of the conceptual security architecture work can be found here: https://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGArchi/Conceptual_Security_Architecture_-_Consensus_Progress.pdf.
    b. We walked through an example of DNP transaction codes: https://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGArchi/Security_Services-And-MessageList-v0p6.xls (tab DNP3 Objects to Msgs)
        i. Thank you to Grant Gilchrist for providing the initial mapping of the DNP transaction codes to our message types.
        ii. The function code is only the beginning. Although the function code is the main intent of the message, the way the 7628 messages have been defined, it's also important to look at the data objects being carried in the message. But even when you consider the objects, the primary problem is that there are several message categories that as defined could map onto any given DNP3 message. In SCADA, for instance, any given binary input object could be considered status, notification, alarm, or alert depending on what the meaning of the binary input was and how the master chose to interpret it. Command and Response are perhaps the worst because almost anything could be considered either a command or response.
        iii. The highlighted items are the "best" mapping to a message while showing all the other possible mappings.
        iv. Question: Do we need to talk about the possibility that a message content may map to multiple message types? Yes. We will need to develop some content to explain this, especially for the DNP3 example.
        v. Question: DNP3 can cross communications to use a TCP/IP stack or proprietary communications, depending upon notable parameters. Can we still apply the DNP3 transactions that cross communications? Yes. We are looking at message/transaction content, so we are not specifying technology or a communication method (we do not want to specify an implementation), this means we can still apply the NISTIR 7628 requirements and allow the utility to select a technology or communication method for their specific implementation.
    c. Using the spreadsheet from SG Network and PAP2, we walk through a sample set of transactions of what a utility will do with their transactions, messages, information within their organization. In creating this sample the following steps were used on the spreadsheet. The sample work can be found here: https://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGArchi/SAMPLE-Payload-LIC-CIA.xls (tab Payload_attrib_LIC_CIA_rtnl)
        i. Note: SGIP PAP2 and CSWG requested that SG Network TF perform a mapping of the Requirement Table payloads to specific NISTIR 7628 security Logical Interface Categories (LIC). This task was accomplished by documenting the following information, where the SG Network TF proposed payload to the NISTIR 7628 LICs are vetted with CSWG and OpenSG SG Security WG. The following describes how the Requirements Table "Payload_attrib_LIC_CIA_rtnl" tab contents are to be documented.
        ii. Payload Name – Copied from the "Reqmts-Combined" tab "Payload Name". Hint, the list of Payload Names is easily created by performing a pivot or datapilot of the "Reqmts-Combined" using "Payload Name" as the primary row element.

iii. Payload Type- Copied from the “Reqmts-Combined” tab “Payload Type”. Hint, the list of Payload Types is easily created by performing a pivot or datapilot of the “Reqmts-Combined” using “Payload Name” and “Payload Type” as the primary and secondary row elements.
iv. Payload Description – Short explanation of what is the application payload use and intent.
v. Payload Attributes – Lists the data elements that are included in the application payload. This excludes any additional security and/or telecommunication protocol(s) added data elements around that application payload. Though not specifically listed, date-time stamps are assumed for all Payloads.
vi. Security LICs - NISTIR 7628 – Logical Interface Category (LIC) derived and mapped (as closely as possible to typically no more than 2-3 LICs) from the NISTIR 7628 document volume 1, section 2.3 “Table 2.2 Logical Interfaces by Category” and remaining sections 2.3.x to the specific application payload in question. Consideration of the originating and consuming actors, specific Domains, telecomm networks used, and application payload content are also necessary in selecting specific LICs. Syntax: [“numeric-alpha value 1” , “numeric-alpha value 2”/”numeric-alpha value n”]
vii. Payload C-I-A Risk Values- Confidentiality, Integrity, Availability security risk levels as described in NISTIR 7628 document volume 1, section 3.2 “Table 3-1 Impact Levels Definitions” and assigned based on the application payload’s description, attributes, C-I-A rationale excluding other security or telecomm network protocol(s) overhead data elements. Syntax (acceptable values): [Confidentiality-risk-level “-“ Integrity-risk-level “-“ Availability-risk-level] where the risk levels have values: L-low; M-moderate; H-high
viii. Security C-I-A Risk Values Rationale – This column is an attempt to document the business impacts of the payload being compromised as assessed against the security confidentiality, integrity, availability areas. Syntax: [“C – “ business impacts and severity due to compromised payload <in cell crt> “I – “ business impacts and severity due to compromised payload <in cell crt> “A – “ business impacts and severity due to compromised payload.

d. Slides from the continued work: https://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGArchi/20120209-SecurityServicesToMessages.ppt
    i. Slide 3. For the drawing showing that there is the potential for a message to cross domain and cross information classification, we need to create text to show this drawing is notional. Suggestion was to use a use case from the service provider or customer domain to show how this is possible and explain the information usage.
    ii. Slide 3. Drawing should be used to explain what we are doing for the conceptual security architecture and why we are not recommending technology for implementation.
    iii. Slide 4 is the potential outline of content for the conceptual security architecture chapter.
        1. We need to expand what will go into the Introduction.
        2. We need to remove the "Conceptual Security Architecture Guiding Principles", because principles are scattered throughout the current NISTIR 7628.
        3. We need to add the examples explaining how to apply the conceptual security architecture to the outline - one for DNP3, one for AMI, and one for cross information classification/cross domain messages.
    iv. Slide 7. On the security services that will be applied to ALL message types, if for a specific implementation non-repudiation is not required or needed, then a requirement needs to be stated that non-repudiation is not required, else requirements are needed for the non-repudiation. We need to put this into an example to ensure the concept is communicated to the reader.
    v. Slide 8. On the security services that will not be applied to ANY message type, we need to put this into an example and use words to describe the why.
    vi. Slide 10. Assigning security services to message types, we will need to put a C-I-A ranking of H-M-L as a minimun security service when applying the NISTIR 7628 requirements and we will need to ensure our examples make sure this point comes across.
e. Looking at the spaghetti drawing, a question was asked about applying security services to the various actors.

i. Our future spaghetti drawing will have layered actors - people, organizations, applications, etc., as well as, a few more actors being added.
ii. Yes, this would be a good idea to add to the conceptual security architecture chapter, because it would allow a utility to look at specific components or actors and see what are the minimum NISTIR 7628 requirements that would apply.

2. Open Items.
    a. On our security services spreadsheet (https://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGArchi/Security_Services-And-MessageList-v0p6.xls) should we change Smart Grid System to Smart Grid Component? Yes.
    b. CSWG F2F, April 25 – 26, Sterling, VA at the Neustar headquarters in Sterling, VA. The first day will be from 8:30 to 5:00, and the second day will be from 8:30 to 1:00. We will be reviewing the NISTIR 7628 chapter 2 updates and the new conceptual security architecture chapter.
3. Attendees
    a. Brian Lenane
    b. Daniel Friedman
    c. Jared Shakespeare
    d. Joe Andrews
    e. Neil Greenfield
    f. Sandy Bacik
    g. Stephen Chasko

Regards,
Sandy Bacik, CISSP, CISM, ISSMP, CGEIT
Principal Consultant
EnerNeX
p: 865.696.4470
e: sandy.bacik@enernex.com // www.enernex.com